Post-quantum Cryptography 101

From basic to attacks

Gustavo Banegas[1]

Technische Universiteit
Eindhoven
University of Technology

March 22, 2018

[1] Department of Mathematics and Computer Science
Technische Universiteit Eindhoven
`gustavo@cryptme.in`

Introduction

- Motivation

Post-quantum cryptography

- PQC Areas
- Code-based cryptography

Quantum Cryptanalysis

Outline

- Introduction
  - Motivation
- Post-quantum cryptography
  - PQC Areas
  - Code-based cryptography
- Quantum Cryptanalysis

Introduction

Motivation

Secure communication

Introduction

Motivation

- Communication channels are spying on our data;

Introduction

Motivation

- Communication channels are spying on our data;
- Communication channels are modifying our data.

Introduction

Motivation

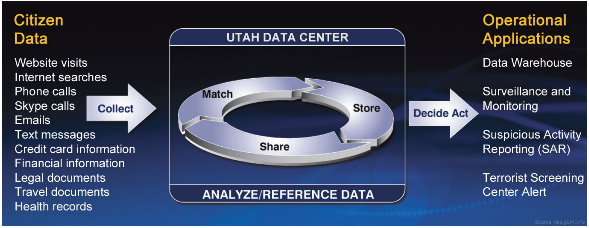
- Communication channels are spying on our data;
- Communication channels are modifying our data.

NATIONAL SECURITY AGENCY
ALL YOUR DATA

Introduction

Should I be concerned?

- Communication channels are storing your data.

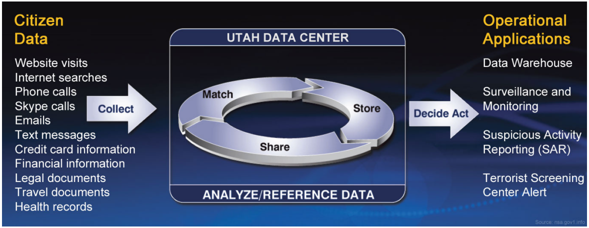


Source: nsa.gov1.info

Introduction

Should I be concerned?

- Communication channels are storing your data.



Citizen Data

Website visits
Internet searches
Phone calls
Skype calls
Emails
Text messages
Credit card information
Financial information
Legal documents
Travel documents
Health records

Collect

UTAH DATA CENTER

Match
Store
Share

ANALYZE/REFERENCE DATA

Decide Act

Operational Applications

Data Warehouse

Surveillance and Monitoring

Suspicious Activity Reporting (SAR)

Terrorist Screening Center Alert

Source: nsa.gov1.info

Introduction

Should I be concerned?

- What they are doing with your data?

Introduction

Should I be concerned?

- What they are doing with your data?
- Are they using just for this purpose?

Introduction

Should I be concerned?

- What they are doing with your data?
- Are they using just for this purpose?
- The history shows: http://www.ibmandtheholocaust.com/

Introduction

Should I be concerned?

- What they are doing with your data?
- Are they using just for this purpose?
- The history shows: http://www.ibmandtheholocaust.com/

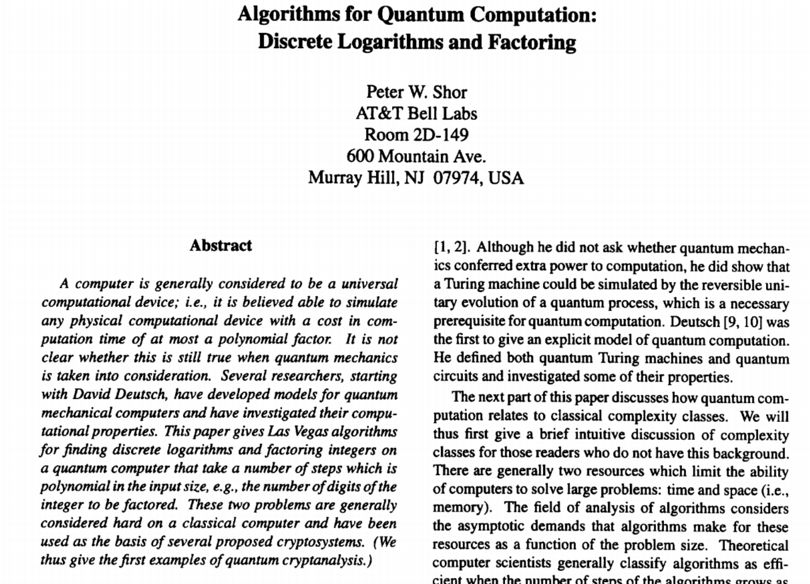
...but I have nothing to hide...

> *"What I want you to do when you get home is email me the passwords to all of your email accounts, not just the nice, respectable work one in your name, but all of them, because I want to be able to just troll through what it is you're doing online, read what I want to read and publish whatever I find interesting. After all, if you're not a bad person, if you're doing nothing wrong, you should have nothing to hide." (Glenn Greenwald)*

It doesn't matter, I am using **Cryptography**.

Introduction

Motivation



Algorithms for Quantum Computation: Discrete Logarithms and Factoring

Peter W. Shor
AT&T Bell Labs
Room 2D-149
600 Mountain Ave.
Murray Hill, NJ 07974, USA

Abstract

A computer is generally considered to be a universal computational device; i.e., it is believed able to simulate any physical computational device with a cost in computation time of at most a polynomial factor. It is not clear whether this is still true when quantum mechanics is taken into consideration. Several researchers, starting with David Deutsch, have developed models for quantum mechanical computers and have investigated their computational properties. This paper gives Las Vegas algorithms for finding discrete logarithms and factoring integers on a quantum computer that take a number of steps which is polynomial in the input size, e.g., the number of digits of the integer to be factored. These two problems are generally considered hard on a classical computer and have been used as the basis of several proposed cryptosystems. (We thus give the first examples of quantum cryptanalysis.)

[1, 2]. Although he did not ask whether quantum mechanics conferred extra power to computation, he did show that a Turing machine could be simulated by the reversible unitary evolution of a quantum process, which is a necessary prerequisite for quantum computation. Deutsch [9, 10] was the first to give an explicit model of quantum computation. He defined both quantum Turing machines and quantum circuits and investigated some of their properties.

The next part of this paper discusses how quantum computation relates to classical complexity classes. We will thus first give a brief intuitive discussion of complexity classes for those readers who do not have this background. There are generally two resources which limit the ability of computers to solve large problems: time and space (i.e., memory). The field of analysis of algorithms considers the asymptotic demands that algorithms make for these resources as a function of the problem size. Theoretical computer scientists generally classify algorithms as efficient when the number of steps of the algorithms grows as

Introduction

- Shor's Algorithm solves in polynomial time:
  - Integer factorization; RSA is dead.
  - The discrete-logarithm problem in finite fields; DSA is dead.
  - The discrete-logarithm problem on elliptic curves; ECDSA is dead.
- Grover's algorithm speeds up brute-force searches.
  - Only 2^{64} quantum operations to break AES-128;
  - 2^{128} quantum operations to break AES-256;

Outline

Introduction

Motivation

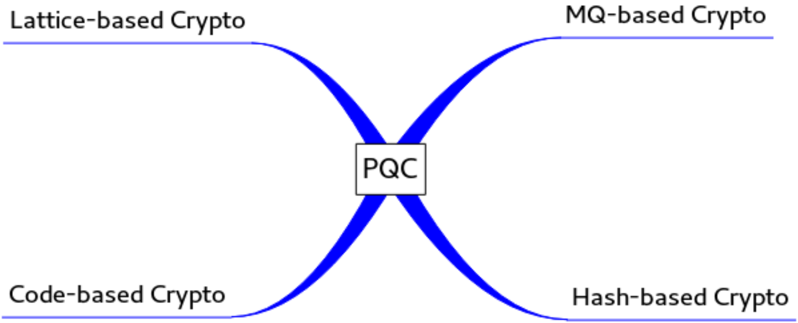
Post-quantum cryptography

PQC Areas

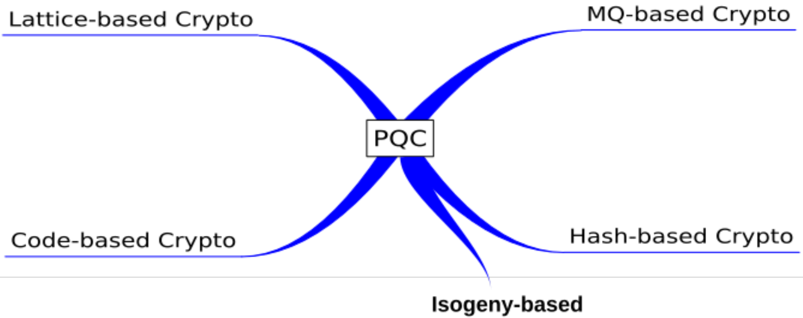
Code-based cryptography

Quantum Cryptanalysis

Overview


Lattice-based Crypto
MQ-based Crypto
PQC
Code-based Crypto
Hash-based Crypto

Overview


Lattice-based Crypto
MQ-based Crypto
PQC
Code-based Crypto
Hash-based Crypto
Isogeny-based

NIST Post-quantum "Competition"

NIST call on PQC

December 2016, after public feedback: NIST calls for submissions of post-quantum cryptosystems to standardize.
30 November 2017: NIST receives 82 submissions.

	Signatures	KEM/Encryption	Overall
Lattice-based	4	24	28
Code-based	5	19	24
MQ-based	7	6	13
Hash-based	4		4
Other	3	10	13
Total	**23**	**59**	**82**

NIST Post-quantum "Competition"

NIST call on PQC

21 December 2017: NIST posts 69 submissions from 260 people. BIG QUAKE. BIKE. CFPKM. Classic McEliece. Compact LWE. CRYSTALS-DILITHIUM. CRYSTALS-KYBER. **DAGS.** Ding Key Exchange. DME. DRS. DualModeMS. Edon-K. EMBLEM and R.EMBLEM. FALCON. FrodoKEM. GeMSS. Giophantus. Gravity-SPHINCS. Guess Again. Gui. HILA5. HiMQ-3. HK17. HQC. KINDI. LAC. LAKE. LEDAkem. LEDApkc. Lepton. LIMA. Lizard. LOCKER. LOTUS. LUOV. McNie. Mersenne-756839. MQDSS. NewHope. NTRUEncrypt. pqNTRUSign. NTRU-HRSS-KEM. NTRU Prime. NTS-KEM. Odd Manhattan. OKCN/AKCN/CNKE. Ouroboros-R. Picnic. pqRSA encryption. pqRSA signature. pqsigRM. QC-MDPC KEM. qTESLA. RaCoSS. Rainbow. Ramstake. RankSign. RLCE-KEM. Round2. RQC. RVB. SABER. SIKE. SPHINCS+. SRTPI. Three Bears. Titanium. WalnutDSA.

Some attack scripts already posted causing total break or serious tweaks.

Many more receiving detailed analysis.

Code-based cryptography

DAGS: Key Encapsulation from Dyadic GS Codes

DAGS is a joint project with:

Gustavo Banegas, Paulo S. L. M. Barreto, Brice Odilon Boidje, Pierre-Louis Cayrel, Gilbert Ndollane Dione, Kris Gaj, Cheikh Thiécoumba Gueye, Richard Haeussler, Jean Belo Klamti, Ousmane N'diaye, Duc Tri Nguyen, Edoardo Persichetti and Jefferson E. Ricardini

https://www.dags-project.org

Code-based cryptography

DAGS: Key Encapsulation from Dyadic GS Codes

DAGS is a joint project with:

Gustavo Banegas, Paulo S. L. M. Barreto, Brice Odilon Boidje, Pierre-Louis Cayrel, Gilbert Ndollane Dione, Kris Gaj, Cheikh Thiécoumba Gueye, Richard Haeussler, Jean Belo Klamti, Ousmane N'diaye, Duc Tri Nguyen, Edoardo Persichetti and Jefferson E. Ricardini

https://www.dags-project.org

Nice.. but "What is code-based cryptography?"

Code-based cryptography

Error correction codes

- Digital media is exposed to memory corruption.
- In general, k bits of data get stored in n bits ($k < n$), adding some redundancy.
- If no error occured, these n bits satisfy $n - k$ parity check equations.

Code-based cryptography

Quick $\mathbb{F}_2$ arithmetic

$\mathrm{GF}(2) = \mathbb{F}_2 = \{0, 1\} = \mathbb{Z}/2$
Addition and multiplication are defined by:

$$0 + 0 = 0 \quad 0 + 1 = 1 \quad 1 + 0 = 1 \quad 1 + 1 = 0$$

$$0 \times 0 = 0 \quad 0 \times 1 = 0 \quad 1 \times 0 = 0 \quad 1 \times 1 = 1$$

It is possible to have $\mathbb{F}_{2^n}$ and polynomial representation $\mathbb{F}_2[x]/f$.
polynomial representation can be defined by:

$$p(x) = \sum_{i=0}^{m} a_i x^i, a_i \in \{0, 1\}$$

Code-based cryptography

Hamming Code

Parity check matrix ($n = 7$, $k = 4$):

$$H = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

An error-free string of 7 bits $\mathbf{b} = \{b_0, b_1, b_2, b_3, b_4, b_5, b_6\}$ satisfies these three equations:

$$\begin{array}{cccccccl} b_0+ & b_1+ & & b_3+ & b_4 & & & = 0 \\ b_0+ & & b_2+ & b_3+ & & b_5 & & = 0 \\ & b_1+ & b_2+ & b_3+ & & & b_6 & = 0 \end{array}$$

If one error occurred at least one of these equations will not hold. Failure pattern uniquely identifies the error location.

Code-based cryptography

Hamming Code

For example, if we have as the result $1, 0, 1$:

$$\begin{aligned} b_0 + b_1 + b_3 + b_4 &= 1 \\ b_0 + b_2 + b_3 + b_5 &= 0 \\ b_1 + b_2 + b_3 + b_6 &= 1 \end{aligned}$$

What does it mean?

Code-based cryptography

Hamming Code

For example, if we have as the result $1, 0, 1$:

$$
\begin{array}{cccccccl}
b_0+ & b_1+ & & b_3+ & b_4 & & & = 1 \\
b_0+ & & b_2+ & b_3+ & & b_5 & & = 0 \\
 & b_1+ & b_2+ & b_3+ & & & b_6 & = 1
\end{array}
$$

What does it mean? bit b_1 flipped.

Code-based cryptography

Coding Theory

Code word $\mathbf{c}$, error vector $\mathbf{e}$, received word $\mathbf{b} = \mathbf{c} + \mathbf{e}$.
Very common to transform the matrix so that the right part has just 1 on the diagonal (no need to store that).

$$H = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \to \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

Given large H, usually very hard to find fast decoding algorithm.

Code-based cryptography

Linear Codes

A binary linear code C of length n and dimension k is a k-dimensional subspace of $\mathbb{F}_2^n$.
C is usually specified as

- the row space of a generating matrix $G \in \mathbb{F}_2^{k \times n}$

$$C = \{mG | m \in \mathbb{F}_2^k\}$$

- the kernel space of a parity-check matrix $H \in \mathbb{F}_2^{(n-k) \times n}$

$$C = \{c | Hc^T = 0, c \in \mathbb{F}_2^k\}$$

“fast” Code-based cryptography 101

Key Generation:

- Choose ω-error correcting code $\mathcal{C}$;
- SK: code description Δ for $\mathcal{C}$;
- PK: generator matrix G in systematic form for $\mathcal{C}$.

“fast” Code-based cryptography 101

Key Generation:

- Choose ω-error correcting code $\mathcal{C}$;
- SK: code description Δ for $\mathcal{C}$;
- PK: generator matrix G in systematic form for $\mathcal{C}$.

Encryption:

- Message is a word $m \in \mathbb{F}_{q^m}^k$;
- Select random error vector $e \in \mathbb{F}_{q^m}^n$ of weight ω;
- $c = mG + e$.

“fast” Code-based cryptography 101

Key Generation:

- Choose ω-error correcting code $\mathcal{C}$;
- SK: code description Δ for $\mathcal{C}$;
- PK: generator matrix G in systematic form for $\mathcal{C}$.

Encryption:

- Message is a word $m \in \mathbb{F}_{q^m}^k$;
- Select random error vector $e \in \mathbb{F}_{q^m}^n$ of weight ω;
- $c = mG + e$.

Decryption:

- Set $m =$Decode(c) and return m;
- Return “fail” if decoding fails.

Code-based cryptography

- 1971 Goppa: Fast decoders for many matrices H.
- 1978 McEliece: Use Goppa codes for public-key cryptography.
- 1986 Niederreiter: Simplified and smaller version of McEliece.
- Security analysis:
  - 1962 Prange; 1981 Omura; 1988 Lee-Brickell; 1988 Leon;
  - 1989 Krouk; 1989 Stern; 1989 Dumer; 1990 Coffey-Goodman;
  - 1990 van Tilburg; 1991 Dumer; 1991 Coffey-Goodman-Farrell;
  - 1993 Chabanne-Courteau; 1993 Chabaud; 1994 van Tilburg;
  - 1994 Canteaut-Chabanne; 1998 Canteaut-Chabaud;
  - 1998 Canteaut-Sendrier; 2008 Bernstein-Lange-Peters;
  - 2009 Bernstein-Lange-Peters-van Tilborg;
  - 2009 Bernstein (post-quantum); 2009 Finiasz-Sendrier;
  - 2010 Bernstein-Lange-Peters; 2011 May-Meurer-Thomae;
  - 2011 Becker-Coron-Joux; 2012 Becker-Joux-May-Meurer;
  - 2015 May-Ozerov;
  - 2013 Bernstein-Jeffery-Lange-Meurer (post-quantum);
  - 2017 Kachigar-Tillich (post-quantum).

Code-based cryptography

Nice codes

- **Generalized Srivastava**;
- Quasi-cyclic codes (QC);
- Quasi-dyadic codes (QD);
- Quasi-Dyadic + Goppa;
- Goppa codes;
- Others. . .

Outline

Introduction

- Motivation

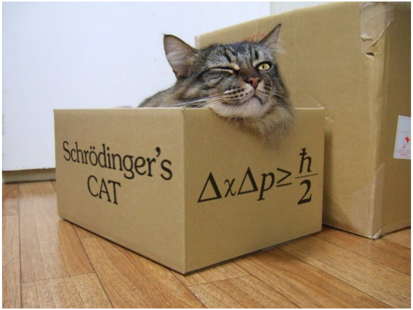
Post-quantum cryptography

- PQC Areas
- Code-based cryptography

Quantum Cryptanalysis

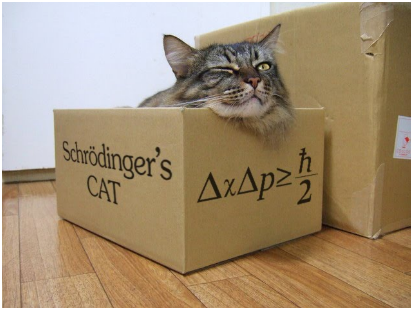
Quantum Computing

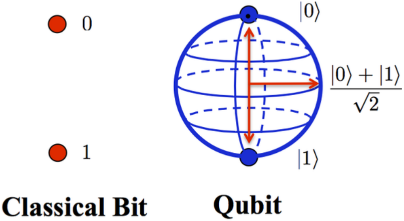
Superposition



Quantum Computing

Superposition





$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Quantum Computing

NCE FAIR
DISQUALIFIED?! IT'S JUST A THOUGHT EXPERIMENT. OBSERVE THE CAT IS FINE!
Schrödinger's Experiment
DISQUALIFIED
Exploring Quantum Entanglement
OPEN
I KNOW WHAT STATE IT SHOULD BE IN...
ANIC
ML

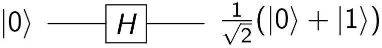
WWW.MARYDEATHCOMICS.COM

Measuring the state collapses the superposition state.

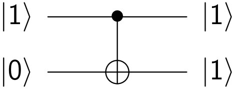
Quantum Computing

Quantum Gates

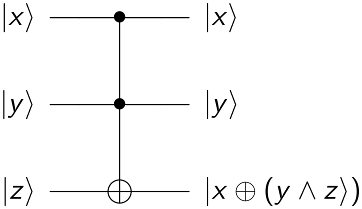
Hadamard gate:



CNot Gate:



Toffoli gate:



All the operations need to be reversible.

Quantum Computing

Deutsch-Jozsa Problem

- Input $f : \{0,1\}^n \to \{0,1\}$ either constant or balanced
- Output: 0 iff f is constant
- Constraints: f is a **black-box**

Query complexity

- Deterministic: $2^{n-1}+1$

Quantum Computing

Deutsch-Jozsa Problem

- Input $f : \{0,1\}^n \to \{0,1\}$ either constant or balanced
- Output: 0 iff f is constant
- Constraints: f is a **black-box**

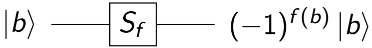
Query complexity

- Deterministic: $2^{n-1} + 1$
- Quantumly: 1

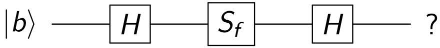
Quantum Computing

Deutsch-Jozsa Algorithm

Implementation of S_f:



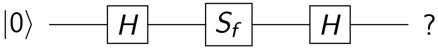
Quantum Circuit:



Quantum Computing

Deutsch-Jozsa Algorithm

Quantum Circuit:



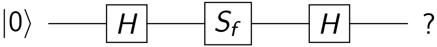
Analysis for 1 qubit:

- Initialization: $|0\rangle$

Quantum Computing

Deutsch-Jozsa Algorithm

Quantum Circuit:



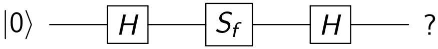
Analysis for 1 qubit:

- Initialization: $|0\rangle$
- Parallelization: $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

Quantum Computing

Deutsch-Jozsa Algorithm

Quantum Circuit:



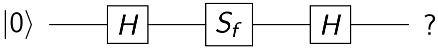
Analysis for 1 qubit:

- Initialization: $|0\rangle$
- Parallelization: $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
- Query: $\frac{1}{\sqrt{2}}((-1)^{f(0)}\,|0\rangle + (-1)^{f(1)}\,|1\rangle)$

Quantum Computing

Deutsch-Jozsa Algorithm

Quantum Circuit:



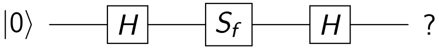
Analysis for 1 qubit:

- Initialization: $|0\rangle$
- Parallelization: $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
- Query: $\frac{1}{\sqrt{2}}((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle)$
- Interferences: $\frac{1}{2}((-1)^{f(0)}(|0\rangle + |1\rangle) + (-1)^{f(1)}(|0\rangle - |1\rangle))$

Quantum Computing

Deutsch-Jozsa Algorithm

Quantum Circuit:



Analysis for 1 qubit:

- Initialization: $|0\rangle$
- Parallelization: $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
- Query: $\frac{1}{\sqrt{2}}((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle)$
- Interferences: $\frac{1}{2}((-1)^{f(0)}(|0\rangle + |1\rangle) + (-1)^{f(1)}(|0\rangle - |1\rangle))$
- Final State:
  $\frac{1}{2}(((-1)^{f(0)} + (-1)^{f(1)})|0\rangle + ((-1)^{f(0)} - (-1)^{f(1)})|1\rangle)$

Quantum World

Quantum Basics

- Qubits
- Quantum Circuits
- Query complexity model
- Quantum Algorithms

Quantum Algorithms

- Deutsch-Jozsa Algorithm
- Simon's Algorithm
  (Quantum period finding)
- Shor's Algorithm
- Grover's Algorithm
- Quantum Walks

Quantum cryptanalysis research retreat (September 2016 2018)
https://www.cryptme.in/events/
Quantum Cryptanalysis - Dagstuhl
https://www.dagstuhl.de/en/program/calendar/semhp/?semnr=17401

Quantum Cryptanalysis

Quantum cryptanalysis

2016 - Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA-3 (Matthew Amy, Olivia Di Matteo, Vlad Gheorghiu, Michele Mosca, Alex Parent, John Schanck)

2017 - Low-communication parallel quantum multi-target preimage search (Gustavo Banegas and Daniel J. Bernstein)

2018 - Improved Quantum Information Set Decoding (Elena Kirshanova)

2018 - Asymptotically faster quantum algorithms to solve multivariate quadratic equations (Daniel J. Bernstein and Bo-Yin Yang)

Questions

Thank you for your attention.
Questions?

gustavo@cryptme.in